In the Claims:

Please amend Claims 1, 3, 10, 13, 16, 22, 53, 54; cancel Claims 4-5, 17-18, 51, and add new Claims 56-62, all as shown below. Applicant respectfully reserves the right to prosecute any originally presented or canceled claims in a continuing or future application.

1.   (Currently Amended) A system for single security administration comprising:

a first [[type]] application server of a first server type, which is configured to execute transaction processes including receiving calls from clients to initiate the transaction processes, wherein the first [[type]] application server includes

an access control list which defines user security information for use in authorizing the calls from clients, and

a Lightweight Directory Access Protocol (LDAP) [[an]] authentication server plugin which is configured to forward the calls from clients to another application server for authorization;

a ~~plurality~~ second application server of a second server type ~~servers, wherein each second-type server includes an embedded server and each second type-server is associated with a security data repository that provides to the second type-server user security information associated with both the first-type server and the second-type server~~ which is configured to administer security for the first application server, wherein the second application server includes

a user profile database which includes security information for a plurality of users, including for each of the users a mapping of security credentials for that user between the first server type and the second server type, and

an embedded LDAP server which is configured to receive the calls from the LDAP authentication server plugin; and

~~wherein the first-type server holds only access control list and relies on one of the plurality of second type-servers to provide user and group information, and,~~

~~wherein, in response to receiving a request for authentication from a user at the first type server, the authentication server at the first type-server determines which second-type-server stores security information for the particular user;~~

wherein, when a call is received from a client to initiate a transaction at the first application server, the LDAP authentication server plugin

identifies the user associated with the call,

determines that the second application server should authenticate the user,

2

initiates an LDAP session between the first [[type]] application server and [[said]] the second [[type]] application server[[;]].

[[passes]] sends a query information from said authentication server to [[said]] the embedded LDAP server[[;]].

receives from the embedded LDAP server a corresponding user information as determined by the user profile database at the second application server[[;]], and

creates a token reflecting the result, which is subsequently used to authenticate the client to participate in the transaction that reflects an authentication result that can be used by said client.

2.   (Canceled).

3.   (Currently Amended) The system of claim 1 wherein said first [[type]] application server is an enterprise server.

4-6.   (Canceled).

7.   (Original) The system of claim 1 wherein said query information is query user information that specifies a particular user or group of users.

8.   (Previously Presented) The system of claim 1 wherein the system includes a plurality of servers.

9.   (Original) The system of claim 8 wherein at least two of said plurality of servers include an LDAP authentication server.

10.   (Currently Amended) The system of claim 1, further comprising a user information cache that caches a copy of said user authentication information in case of a failure in a communication link between the first [[type]] application server and the second [[type]] application [[of]] server.

11.   (Original) The system of claim 1 wherein the system is scalable to include multiple LDAP authentication servers and/or multiple embedded LDAP servers.

3

Attorney Docket No.: ORACL-01416US1 SRM/KRL
M:\tliu\wp\ORACL\1400-1499\1416US1\oracl_1416us1_Reply_061809_OA.doc

PAGE 5/16 * RCVD AT 11/18/2009 8:08:07 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-5/38 * DNIS:2738300 * CSID:415 362 2928 * DURATION (mm-ss):03-16

12.   (Original) The system of claim 1 wherein at least one of said servers include a console program for administering the security of the system.

13.   (Currently Amended) A method for providing single security administration comprising the steps of:

providing a first application server of a first server type, which is configured to execute transaction processes including receiving calls from clients to initiate the transaction processes, wherein the first server includes

an access control list which defines user security information for use in authorizing the calls from clients, and

a Lightweight Directory Access Protocol (LDAP) authentication server plugin which is configured to forward the calls from clients to another application server for authorization;

providing a second application server of a second server type, which is configured to administer security for the first application server, wherein the second application server includes

a user profile database which includes security information for a plurality of users, including for each of the users a mapping of security credentials for that user between the first server type and the second server type, and

an embedded LDAP server which is configured to receive the calls from the LDAP authentication server plugin;

receiving a call from a client to initiate a transaction at the first application server; and

performing, via the LDAP authentication server plugin, the steps of

identifying the user associated with the call,

determining that the second application server should authenticate the user,

initiating a LDAP session between the first application server and the second application server,

sending a query information to the embedded LDAP server,

receiving from the embedded LDAP server a corresponding user information as determined by the user profile database at the second application server, and

creating a token reflecting the result, which is subsequently used to authenticate the client to participate in the transaction

4

issuing a call to an authentication server at a first-type server, wherein the first-type server holds only access control list and relies on one of the plurality of second-type servers to provide user and group information;

determining which second-type server stores security information for the particular user;

passing query user information from said authentication server to an embedded LDAP server at the second-type server, wherein the second-type server includes a single security data repository that provides the second-type server user-security information associated with both the one of the first-type servers and the second-server;

returning corresponding user information to said authentication server; and,

providing an authentication token for use by the client.

14. (Original) The method of claim 13, further comprising the step, prior to issuing a call, of allowing a client to access a default security plugin.

15. (Canceled).

16. (Currently Amended) The method of claim 13 wherein said first [[type]] application server is an enterprise server.

17-19. (Canceled).

20. (Previously Presented) The method of claim 13 wherein said query user information is query user information that specifies a particular user or group of users.

21. (Previously Presented) The method of claim 13, further comprising: including a plurality of servers.

22. (Currently Amended) The method of claim 21 wherein at least two of said plurality of servers include [[an]] a LDAP authentication server.

23. (Original) The method of claim 13, further comprising a user information cache that caches a copy of said user information.

24. (Previously Presented) The method of claim 13, further comprising:

5

being scalable to include multiple LDAP authentication servers and/or multiple embedded LDAP servers.

25.   (Original) The method of claim 13 wherein at least one of said servers include a console program for administering the security of the system.

26-51.   (Canceled).

52.   (Previously Presented) The system of claim 1, wherein:

the session is a LDAP session that supports a single user security data store and administration.

53.   (Currently Amended) The system of claim 1, wherein:

each of the plurality of the second application server type of servers supports backup or failover authentication.

54.   (Currently Amended) The system of claim 1, wherein:

the first [[type]] application server also supports a separate independent authentication mechanism with a separate security repository.

55.   (Previously Presented) The system of claim 53, further comprising:

a migrating utility that takes user security information from the separate security repository associated with the first type server and updates the security data repository associated with at least one of the plurality of second type servers.

56.   (New) The system of claim 1, wherein:

the LDAP authentication server plugin at the first application server further

determines another second type server in a plurality of second type servers that stores user and group information for a particular user, when a previously determined second type server fails,

initiates a session between the first application server and said another second type server,

passes query information from said authentication server to an embedded LDAP server in said another second type server, and

6

receives corresponding user and group information from the embedded LDAP server in said another second type server.

57.   (New) The system of claim 1 wherein the first server type and first application server are Tuxedo-based, and the second server type and second application server are a type other than Tuxedo.

58.   (New) The method of claim 13, wherein:

performing,via the LDAP authentication server plugin, the steps of

determining another second type server in a plurality of second type servers that stores user and group information for a particular user, when a previously determined second type server fails,

initiating a session between the first application server and said another second type server,

passing query information from said authentication server to an embedded LDAP server in said another second type server, and

receiving corresponding user and group information from the embedded LDAP server in said another second type server.

59.   (New) The method of claim 13 wherein the first server type and first application server are Tuxedo-based, and the second server type and second application server are a type other than Tuxedo.

60.   (New) A machine readable storage medium having instructions embedded thereon and performing the following functions when executed by a processor:

providing a first application server of a first server type, which is configured to execute transaction processes including receiving calls from clients to initiate the transaction processes, wherein the first application server includes

an access control list which defines user security information for use in authorizing the calls from clients, and

a Lightweight Directory Access Protocol (LDAP) authentication server plugin which is configured to forward the calls from clients to another application server for authorization;

providing a second application server of a second server type, which is configured to

7

Attorney Docket No.: ORACL-01416US1 SRM/KRL
M:\tlu\wp\ORACL\1400-1499\1416US1\oracl_1416us1_Reply_061809_OA.doc

PAGE 9/16 * RCVD AT 11/18/2009 8:08:07 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-5/38 * DNIS:2738300 * CSID:415 362 2928 * DURATION (mm-ss):03-16

administer security for the first application server, wherein the second application server includes

a user profile database which includes security information for a plurality of users, including for each of the users a mapping of security credentials for that user between the first server type and the second server type, and

an embedded LDAP server which is configured to receive the calls from the LDAP authentication server plugin;

receiving a call from a client to initiate a transaction at the first application server; and

performing, via the LDAP authentication server plugin, the steps of

identifing the user associated with the call,

determining that the second application server should authenticate the user,

initiating a LDAP session between the first application server and the second application server,

sending a query information to the embedded LDAP server,

receiving from the embedded LDAP server a corresponding user information as determined by the user profile database at the second application server, and

creating a token reflecting the result, which is subsequently used to authenticate the client to participate in the transaction.

61.   (New) The machine readable storage medium of claim 60, further comprising instructions performing the following functions when executed by a processor:

performing, via the LDAP authentication server plugin, the steps of

determining another second type server in a plurality of second type servers that stores user and group information for a particular user, when a previously determined second type server fails,

initiating a session between the first application server and said another second type server,

passing query information from said authentication server to an embedded LDAP server in said another second type server, and

receiving corresponding user and group information from the embedded LDAP server in said another second type server.

8

Attorney Docket No.: ORACL-01416US1 SRM/KRL
M:\tliu\wp\ORACL\1400-1499\1416US1\oracl_1416us1_Reply_061809_OA.doc

PAGE 10/16 * RCVD AT 11/18/2009 8:08:07 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-5/38 * DNIS:2738300 * CSID:415 362 2928 * DURATION (mm-ss):03-16

62.   (New) The machine readable storage medium of claim 60, wherein the first server type and first application server are Tuxedo-based, and the second server type and second application server are a type other than Tuxedo.

9